REMARKS

Applicant cancels claim 20 directed to a carrier wave signal, which, in spite of applicant arguments expressed in the 05/02/07 Amendment, was again rejected by the Office Action mailed on 07/24/2007, based on 35 U.S.C. 101 as non patentable subject matter. However, applicant is not conceding that a carrier wave signal is not patentable subject matter. Claim 20 is canceled only for facilitating expeditious prosecution of clams 1, 4-8, 10-15, 18, and 19. Applicant respectfully reserves the right to pursue claim 20, and other claims, directed to a carrier wave signal in one or more continuations and/or divisional patent applications.

Office Action (OA) mailed on 07/24/2007, also rejected claims 1, 4-8, 10-15, and 18-20 under 35 U.S.C. 103(a) as being unpatentable over Oskari U.S. Patent Publication No. 2006/0072755 (hereinafter '755) in view of Kung U.S. Patent 5,442,342 (hereinafter '342).

OA states: "As to independent claim 1, *"A portable computing device for opening a door, comprising: a memory, wherein a content of the memory comprises: a first copy of a shared secret key; a first standard certificate, wherein the first standard certificate is being used in responding to a challenge of the door"* is taught in '755 page 3, paragraphs 0052-0053; "*and means for communicating with the door, wherein the door possesses a second copy of the shared secret key, and wherein the door adapted to validate identicalness of the first and the second copies of the shared secret key*" is shown in '755 page 2, paragraphs 0058-0061;"

Applicant would respectfully argue that first and second copies of shared secret key are not taught in '755 at all. Document '755 is dealing exclusively with public key cryptography, namely with its implementation in Bluetooth technology. Applicant would respectfully advance the point of view that the OA simply misunderstood claim 1, '755, and in general, the difference between asymmetric public key, and symmetric private key cryptography.

The instant invention teaches, and claim 1 is directed to, a particular combination of private secret key and public public/private key cryptography, which combination aims to achieve an optimal tradeoff between security and computational complexity. The portable computing device of claims 1, 4, and 10 has both a private secret key, and the private (or public) key of a standard certificate. The term standard certificate is a common use expression for public key encryption.

It is an unfortunate nomenclature that one of the keys of public system is called “private” or “secret”, the same name as the whole secret-key symmetric encryption scheme is referred to. But, they are drastically different concepts. These are abundantly described in the instant invention, for instance, when discussing Figs. 1 and 2, on pages 6 to 9.

Paragraph 0053 of ‘755 states: “The encryption uses an encryption key pair system, with the public key being carried in the lock and the private key being carried in the key.”
This is the quintessential application of public key cryptography, and there is nothing in paragraph 0053, or anywhere in ‘755, about private secret keys. The “secret, or private, key” of ‘755 is not the secret key of claims 1, 4, and 10. The “public key / private key” of ‘755 is the “standard certificate” of the instant invention, and of claims 1, 4, and 10.

Public-key versus secret-key cryptography are well known concepts in the encryption arts. For instance, applicant needs to refer only such a readily accessible source as Wikipedia on the Internet. Just going to the main page: <http://en.wikipedia.org/wiki/Main_Page> and searching for the word: “encryption” brings up all the relevant information.

For instance, the page: <http://en.wikipedia.org/wiki/Encryption> contains the following paragraph: “Modern encryption methods can be divided into symmetric key algorithms (Private-key cryptography) and asymmetric key algorithms (Public-key cryptography). In a symmetric key algorithm (e.g., DES and AES), the sender and receiver must have a shared key set up in advance and kept secret from all other parties; the sender uses this key for encryption, and the receiver uses the same key for decryption. In an asymmetric key algorithm (e.g., RSA), there are two separate keys: a public key is published and enables any sender to perform encryption, while a private key is kept secret by the receiver and enables only him to perform correct decryption.” (Underlines done by applicant.) Sites like: <http://en.wikipedia.org/wiki/Symmetric-key_cryptography> and

<http://en.wikipedia.org/wiki/Public-key_cryptography> can be linked from the "Encryption" page, wherein the state of the prior art is clarified in great detail. It is also explained why for public/private keys in the public-key system one relies on standard certification, as it is used in the instant invention.

Secret-key, or private-key, cryptography has been around since ancient times, while public key cryptography emerged in 1976. The specification of the instant invention explains the use of each in the embodiments of the invention. For instance, commencing on page 2 line 16 to page 3 line 13 the basic rationale is given why to use both the public public/private encryption with standard certificates, and the private secret key encryption.

Returning to the cited documents, just to point out another glaring example of '755 use of only customary public-key cryptography, is their short paragraph 0066. This is the list of the used keys, and it says: "An RSA key pair." RSA is the most widely used public-key encryption system, with a public and private key. Paragraph 0004 of '755 describes the pitfalls of secret keys (in the opinion of '755 inventors), in order to set up the use of public-key encryption in that disclosure.

The other cited documents of the OA: '342, and Zuili US Patent No.: 7,083,090, have nothing, as well, on combining the robustness of public-key cryptography with the speed and simplicity of shared secret private-key cryptography.

Accordingly, applicant would respectfully aver that the claims of the instant invention, as expressed in applicants 05/02/07 Amendment, are not rendered obvious by the cited documents, and are patentable.

Applicant respectfully submits that with claim 20 canceled this application is in condition for allowance, which action is respectfully requested.

Respectfully,

George Sai-Halasz, PhD
Registration # 45,430

303 Taber Avenue
Providence, RI 02906
T: 401-427-0853, Fax 401-427-0319
E-MAIL - patents@computer.org

Cust. No.: **24299**